UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/755,668	01/13/2004	Denis Bisson	14296-27	9623

77130 7590 05/12/2008

LABTRONIX CONCEPT
C/O BENOIT & CO INC.
2025 LIMOGES
LONGUEUIL, QC J4G 1C4
CANADA

EXAMINER	
DADA, BEEMNET W	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
05/12/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/755,668	BISSON ET AL.	
	Examiner	Art Unit	
	BEEMNET W. DADA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 January 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-57* is/are pending in the application.

4a) Of the above claim(s) *14-35 and 50-57* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13 and 36-49* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This office action is in reply to an amendment filed on January 28, 2008. Claims 1-57 are pending.

Response to Arguments

Applicant's arguments with respect to claim 1 has been considered but are moot in view of the new ground(s) of rejection.

Applicant's arguments filed 01/28/08 with respect to combination of Shimizu and Al-Salqan have been fully considered but they are not persuasive. Applicant argues that the goal of the two systems are very different and it would not be obvious to someone of ordinary skill in the art at to enhance the security of Shimizu with something taught by Al-Salqan. Examiner disagrees.

Examiner would point out that a suggestion, teaching, or motivation to combine the relevant prior art teachings does not have to be found explicitly in the prior art, as the teachings, motivation, or suggestion may be implicit from the prior art, as a whole, rather than expressly stated in the references. The test for an implicit showing is what the combined teachings, knowledge of one of a whole would have suggested to those of ordinary skill in the art. In re Kahn, 441 F.3d 977, 988, 78, USPQ2d 1329, 1336 (Fed. Cir. 2006) citing In re Kotzab, 217 F.3d 1365,1370, 55 USPQ2d 1313 (Fed. Cir. 2000). See also In re Thrift, 298 F. 3d 1357, 1363, 63 USPQ2d 2002, 2008 (Fed. Cir. 2002). These showings by the examiner are an essential part of complying with the burden of presenting a prima facie case of obviousness. Note In re Oetiker, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). In this case the concept of storing a public key, encrypting/decrypting a correspondent key identifier (i.e., key recovery information) using said public key thereby extracting the corresponding key identifier as taught

by Al-Salqan could be employed within the system of Shimizu in order to enhance the security of the system.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shimizu et al. US 6,085,323 (hereinafter Shimizu) in view of Al-Salqan (US 6,775,382 B1) and further in view of Schneier et al. US 7,362,862 B2 (hereinafter Schneier).

As per claim 1, Shimizu teaches a method of transmitting data using encryption between a sender and a receiver, the method comprising:

generating a first encryption key unknown to the receiver (i.e., random number generator 3 of fig1, column 7, lines 4-7);

encrypting said data to be transmitted from the sender to the receiver using said first key (i.e., encrypting device 4, of fig 1, column 7, lines 10-13);

providing separate Second Information Processing Systems (SIPSs) in secure local communication with both the sender and the receiver [figures 1-3];

the sender transmitting to its SIPS the first encryption key and information dependent on an identity of the receiver, the SIPS of the sender selecting one of a plurality of second keys corresponding to the information dependent on the identity of the receiver and a unique an identifier corresponding to said selected second key, said identifier and said corresponding

selected second key being known to the SIPS of the receiver (i.e., key selection, column 14, lines 15-30);

the SIPS of the sender encrypting the first encryption key using the selected second key to provide an encrypted first key (i.e., encrypting temporary key using master key, column 7, lines 13-21 and column 14, lines 22-30);

transmitting said encrypted first key, said identifier and said data to be transmitted from the sender to the receiver using said first key over a generally unsecured transmission link [column 7, lines 17-22 and lines 39-49 and fig 1-3];

transmitting from the receiver to the SIPS of the receiver said encrypted first key and said identifier [column 7, lines 17-22 and lines 39-49];

the SIPS of the receiver decrypting said encrypted first key using said second encryption key to provide the receiver with the first encryption key [column 8, lines 7-19 and column 1`5, lines 14-35]; and

the receiver decrypting said data using said the retrieved first encryption key [column 8, lines 7-19 and column 15, line 54-column 16, line 6]. Shimizu further teaches SIPS identification means to identify a correspondent key and a correspondent key identifier. Shimizu is silent on the method including the steps of encrypting correspondent key identifier using a public key to generate a secured key identifier. Al-Salqan teaches a system for recovering encryption keys, including storing a public key, encrypting/decrypting a correspondent key identifier (i.e., key recovery information) using said public key thereby extracting the corresponding key identifier [column 2, lines 65-column 3, line 10]. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Al-Salqan within the system of Shimizu in order to enhance the security of the system.

The combination of Shimizu and Al-Salqan is silent on selection of keys based on unique identifier. However such method is well known in the art which has the advantage of enhancing security of the system. For example, Schneier teaches an authentication system including selection of different keys based on a unique identification of a system [column 47, lines 43-50]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Schneier within the system of Shimizu and Al-Salqan in order to enhance the security of the system.

Claims 2-13 and 36-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shimizu et al. US 6,085,323 (hereinafter Shimizu) in view of Al-Salqan (US 6,775,382 B1).

As per claims 2, 36 and 45, Shimizu teaches an information process arrangement comprising a First Information Processing System (FIPS) and a Second Information Processing System (SIPS) arranged separate from the FIPS and capable of exchanging signals with the FIPS [see figures 1-3], wherein the FIPS comprises

FIPS key generation means to generate a first key (i.e., random number generator 3 of fig1, column 7, lines 4-7);

FIPS encryption means to encrypt sensitive data using the first key, thereby generating temporarily secured sensitive data (i.e., encrypting device 4, of fig 1, column 7, lines 10-13); FIPS correspondent selection means to select correspondent data to which the sensitive data is destined (i.e., selection of user or group, column 14, lines 15-22); and

FIPS storage means to store temporarily secured sensitive data (i.e., storage device 12 of fig 1);

the SIPS comprises SIPS storage means to store correspondence data, a plurality of keys, a plurality of key identifiers (i.e., IC Card, 5 of figure 1, column 14, lines 4-15); SIPS identification means to identify a correspondent key and a correspondent key identifier based on received FIPS selected correspondent data (i.e., key selection, column 14, lines 15-30); and SIPS encryption means to encrypt FIPS received first key using said identified correspondent key, and thereby generating a secured first key (i.e., encrypting temporary key using master key, column 7, lines 13-21 and column 14, lines 22-30);

the FIPS further comprises FIPS secured data integration means to integrate into temporarily secured sensitive data, received SIPS secured first key and integrated secured sensitive data [column 7, lines 17-22 and lines 39-49]. Shimizu further teaches SIPS identification means to identify a correspondent key and a correspondent key identifier. Shimizu is silent on the method including the steps of encrypting correspondent key identifier using a public key to generate a secured key identifier. Al-Salqan teaches a system for recovering encryption keys, including storing a public key, encrypting a correspondent key identifier (i.e., key recovery information) using said public key thereby generating a secured key identifier [column 2, lines 65-column 3, line 10]. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Al-Salqan within the system of Shimizu in order to enhance the security of the system.

As per claims 9, 41 and 48, Shimizu teaches an information process arrangement comprising a First Information Processing System (FIPS) and a Second Information Processing System (SIPS) arranged separate from the FIPS and capable of exchanging signals with the FIPS, wherein the FIPS comprises

FIPS storage means to store integrated secured sensitive data (i.e., storage device 12 of fig 1); and

FIPS secured data extraction means to extract from integrated secured sensitive data a secured first key, a secured key identifier, and temporarily secured sensitive data (i.e., key selection, column 14, lines 15-30);

the SIPS comprises SIPS storage means to store correspondence data, a plurality of keys, a plurality of key identifiers (i.e., IC Card, 5 of figure 1, column 14, lines 4-15);

SIPS decryption means to decrypt FIPS received secured first key using the key corresponding in the SIPS storage means to extracted key identifier, thereby extracting the first key [column 8, lines 7-19 and column 1`5, lines 14-35]; and

the FIPS further comprises FIPS decryption means to decrypt temporarily secured sensitive data using the SIPS received first key, therefore extracting the sensitive data [column 8, lines 7-19 and column 15, line 54-column 16, line 6]. Shimizu further teaches SIPS identification means to identify a correspondent key and a correspondent key identifier. Shimizu is silent on the method including the steps of encrypting correspondent key identifier using a public key to generate a secured key identifier. Al-Salqan teaches a system for recovering encryption keys, including storing a public key, encrypting/decrypting a correspondent key identifier (i.e., key recovery information) using said public key thereby extracting the corresponding key identifier [column 2, lines 65-column 3, line 10]. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Al-Salqan within the system of Shimizu in order to enhance the security of the system.

As per claims 3, 10, 37, 42, 46 and 49, Shimizu further teaches the system further comprising authentication means receiving user provided authentication data which is compared with SIPS stored authentication data in order to grant or deny SIPS use [column 7, lines 4-21].

As per claims 4, Shimizu further teaches the system wherein the SIPS further comprises integration means to integrate SIPS encrypted data in a single signal communicated to the FIPS [column 7, lines 4-21 and figures 1-3].

As per claims 5, 11, 39 and 44, Shimizu further teaches the system wherein the FIPS further comprises at least one of: communication control means to close external communication when a securing sensitive data process is initiated, anti-spy means to prevent undesired means to record signal exchanged between the FIPS and the SIPS, and automatic deletion means to erase from the FIPS at least one of unsecured, FIPS secured and SIPS secured data else that integrated secured sensitive data one the integrated secured sensitive data has been generated [column 7, lines 4-21 and figures 1-3].

As per claims 6, 12, 40 and 47, Shimizu further teaches the system wherein the SIPS further comprises puzzling means that complete at least one of: creating unnecessary signals between valuable signals transmitted to the FIPS, and modifying SIPS generated signals and data transmitted to the FIPS in order to render more difficult the reading of said signals and data [column 7, lines 4-21 and figures 1-3].

As per claim 7, Shimizu further teaches the system wherein a second processing arrangement having a SIPS component having stored correspondent key and associated

correspondent key identifier corresponding to the information processing arrangement SIPS stored selected correspondent key and correspondent key identifier is necessary to decrypt the integrated secured sensitive data generated by the information processing arrangement [column 7, lines 4-21 and figures 1-3].

As per claims 8 and 13, Shimizu further teaches the system wherein the FIPS is a data processing system including communication capability and the FIPS is a smart card comprising computing capability [column 7, lines 4-21 and figures 1-3].

As per claim 38 and 43, Shimizu further teaches the system further comprising at least one of: storing integrated secured data on accessible holding means and communicating integrated secured data to a correspondent FIPS [column 7, lines 4-29].

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BEEMNET W. DADA whose telephone number is (571)272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Beemnet W Dada/
Art Unit 2135

May 8, 2008